UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

ALEXIS DOUGHERTY, DENNIS CALABRESE, LILY NICOLE PORTEE, JESSIE RUIZ-JACOBS, PETER BUNGERT, CHRISTIE STARNES, KASSANDRA BLANKENSHIP, JAMES HIGGINS, and LEONARDO YON, on behalf of themselves and all others similarly situated, Plaintiffs, v. **BOJANGLES' RESTAURANTS, INC.**, Defendant.	No. 3:25-cv-00065 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Alexis Dougherty, Dennis Calabrese, Lily Nicole Portee, Jessie Ruiz-Jacobs, Peter Bungert, Christie Starnes, Kassandra Blankenship, James Higgins, and Leonardo Yon ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant Bojangles' Restaurants, Inc. ("Bojangles" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsels' investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a fast-food chain "specializing in craveable Southern chicken, biscuits and tea" and has approximately 800 locations across 17 states.[1]

[1] *About Us*, BOJANGLES, https://www.bojangles.com/about (last visited Jan. 2, 2025).

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its current and former employees. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former employees' PII/PHI.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiffs are Data Breach victims, having received a breach notice. They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII/PHI to cybercriminals is a bell that cannot be unrung. Before this data breach, its current and former employees' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff Alexis Dougherty is a natural persona and citizen of North Carolina where she intends to remain.

9. Plaintiff Dennis Calabrese is a natural persona and citizen of North Carolina where he intends to remain.

10. Plaintiff Lily Nicole Portee is a natural person and citizen of South Carolina where she intends to remain.

11. Plaintiff Jessie Ruiz-Jacobs is a natural person and citizen of North Carolina where he intends to remain.

12. Plaintiff Peter Bungert is a natural person and citizen of Texas where he intends to remain.

13. Plaintiff Christie Starnes is a natural person and citizen of North Carolina where she intends to remain.

14. Plaintiff Kassandra Blankenship is a natural person and citizen of Tennessee where she intends to remain.

15. Plaintiff James Higgins is a natural person and citizen of North Carolina, where he intends to remain.

16. Plaintiff Leonardo Yon is a natural person and citizen of North Carolina where he intends to remain.

17. Defendant, Bojangles' Restaurants, Inc., is a corporation incorporated in Delaware and with its registered address at 160 Mine Lake Court, Raleigh, North Carolina 27615

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states. And there are over 100 putative Class Members.

19. This Court has personal jurisdiction over Defendant because it is headquartered in North Carolina, regularly conducts business in North Carolina, and has sufficient minimum

contacts in North Carolina.

20. Venue is proper in this Court because a substantial part of events or omissions giving rise to the cause of action occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiffs and the Class

21. Defendant is a fast-food chain "specializing in craveable Southern chicken, biscuits and tea" and has approximately 800 locations across 17 states.[2]

22. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former employees.

23. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their PII/PHI.

24. Under state and federal law, businesses like Defendant have duties to protect its current and former employees' PII/PHI and to notify them about breaches.

25. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

a. "Bojangles has security policies and practices in place designed to protect your Personal Information against unauthorized access or disclosure, theft, misuse, and loss."[3]

b. "We make commercially reasonable efforts for secure handling of this information[.]"[4]

[2] *About Us*, BOJANGLES, https://www.bojangles.com/about (last visited Jan. 2, 2025).
[3] *Privacy Policy*, BOJANGLES (June 1, 2021) https://www.bojangles.com/privacy-policy.
[4] *Id*.

Defendant's Data Breach

26. From February 19, 2024, through March 12, 2024, Defendant was hacked in the Data Breach.[5]

27. Worryingly, Defendant already admitted that its "investigation subsequently determined that certain files were viewed and downloaded by an unknown actor between February 19, 2024 and March 12, 2024."[6]

28. Because of Defendant's Data Breach, at least the following types of PII/PHI were compromised:

a. names;

b. addresses;

c. Social Security numbers;

d. driver's license numbers;

e. government-issued ID numbers;

f. passport numbers;

g. state ID numbers;

h. financial information;

i. financial account numbers;

j. credit card numbers;

k. debit card numbers;

l. health insurance information; and

[5] *Notice of Data Event*, NEW HAMPSHIRE ATTY GEN (Nov. 19, 2024) https://mm.nh.gov/files/uploads/doj/remote-docs/bojangles-restaurants-20241119.pdf.
[6] *Id*.

m. medical information.[7]

29. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative class is over one hundred members—as it includes its current and former employees.

30. And yet, Defendant waited over until November 19, 2024, before it began notifying the class—a full 274 days after the Data Breach began.[8]

31. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

32. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

a. "We encourage you to remain vigilant against incidents of identity theft by reviewing account statements and credit reports for unusual activity and to detect errors."[9]

b. "We also encourage you to review the information contained in the enclosed Steps You Can Take to Help Protect Personal Information."[10]

c. "Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps consumers can take to protect personal

[7] *Data Security Breach Reports*, ATTY GEN TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Jan. 2, 2025).
[8] *Notice of Data Event*, NEW HAMPSHIRE ATTY GEN (Nov. 19, 2024) https://mm.nh.gov/files/uploads/doj/remote-docs/bojangles-restaurants-20241119.pdf.
[9] *Id.*
[10] *Id.*

> information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general."[11]

33. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

34. Since the breach, Defendant claims to have "reviewed our existing policies and procedures" and "enhanced certain administrative and technical controls[.]"[12] But such simple declarations are insufficient to ensure that Plaintiffs' and Class Members' PII/PHI will be protected from additional exposure in a subsequent data breach.

35. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and Class Members for the injuries that Defendant inflicted upon them.

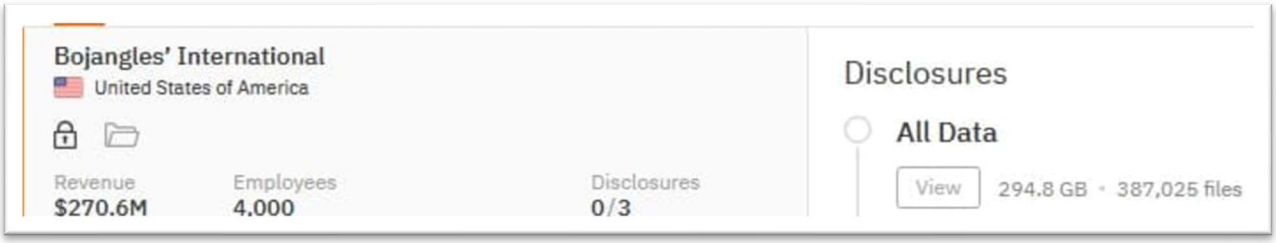
36. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiffs and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class Members.

37. Worryingly, the cybercriminals that obtained Plaintiffs' and Class Members' PII/PHI appear to be the notorious cybercriminal group "Hunters."[13]

---

[11] *Id.*
[12] *Id.*
[13] Paul Bischoff, *Fried chicken chain Bojangles breached; SSNs and medical info stolen by ransomware gang*, COMPARITECH (Nov. 21, 2024) https://www.comparitech.com/news/fried-chicken-chain-bojangles-breached-ssns-and-medical-info-stolen-by-ransomware-gang/.

38. Here, Hunters posted on its Dark Web webpage that it had exfiltrated "387,025 files" which equates to "294.8 GB" of data.[14] A screenshot of the Dark Web webpage is reproduced below.



39. Still, despite this public evidence of broad misuse, Defendant misleadingly claims that "we have no indication of identity theft or fraud in relation to this event[.]"[15]

40. Thus, on information and belief, Plaintiffs' and the Class's stolen PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff Alexis Dougherty's Experience and Injuries

41. Plaintiff Alexis Dougherty is a former employee of Defendant.

42. Thus, Defendant obtained and maintained Plaintiff Dougherty's PII/PHI.

43. As a result, Plaintiff Dougherty was injured by Defendant's Data Breach.

44. As a condition of her employment with Defendant, Plaintiff Dougherty provided Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII/PHI in order to obtain employment and payment for that employment.

45. Plaintiff Dougherty provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain her PII/PHI and has a

[14] *Id.*
[15] *Notice of Data Event*, NEW HAMPSHIRE ATTY GEN (Nov. 19, 2024) https://mm.nh.gov/files/uploads/doj/remote-docs/bojangles-restaurants-20241119.pdf.

continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

46. Plaintiff Dougherty reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

47. Plaintiff Dougherty received a Notice of Data Breach in November 2024.

48. Thus, on information and belief, Plaintiff Dougherty's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

49. Through its Data Breach, Defendant compromised Plaintiff Dougherty's PII/PHI.

50. Plaintiff Dougherty has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed her to take those steps in its breach notice.

51. And in the aftermath of the Data Breach, Plaintiff Dougherty has suffered from a spike in spam and scam phone calls since February 2024.

52. Plaintiff Dougherty fears for her personal financial security and worries about what information was exposed in the Data Breach.

53. Because of Defendant's Data Breach, Plaintiff Dougherty has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Dougherty's injuries are precisely the type of injuries that the law contemplates and addresses.

54. Plaintiff Dougherty suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

55. Plaintiff Dougherty suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that

Defendant was required to adequately protect.

56. Plaintiff Dougherty suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed her PII/PHI right in the hands of criminals.

57. Because of the Data Breach, Plaintiff Dougherty anticipates spending considerable amounts of time and money to try and mitigate her injuries.

58. Today, Plaintiff Dougherty has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Dennis Calabrese's Experience and Injuries

59. Plaintiff Calabrese is a former employee at Defendant.

60. As a condition of his employment at Defendant, he was required to provide Defendant with his sensitive PII, including his Social Security number.

61. Plaintiff Calabrese received a notice letter from Defendant dated November 19, 2024, informing him that his PII—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

62. Plaintiff Calabrese is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

63. At the time of the Data Breach, Defendant retained Plaintiff Calabrese's PII in its system.

64. Plaintiff Calabrese would not have provided his PII to Defendant had he known that Defendant would not utilize standard measures to reasonably secure his sensitive.

65. Because of the Data Breach, Plaintiff Calabrese's PII is now in the hands of cyber

criminals. Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

66. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, researching how best to ensure that he is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach.

67. Plaintiff Calabrese has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

68. The Data Breach has caused Plaintiff Calabrese to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

69. As a result of the Data Breach, Plaintiff Calabrese anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

70. As a result of the Data Breach, Plaintiff Calabrese is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Lily Nicole Portee's Experiences and Injuries

71. Plaintiff Lily Nicole Portee is a former employee of Defendant.

72. Thus, Defendant obtained and maintained Plaintiff Portee's PII/PHI.

73. As a result, Plaintiff Portee was injured by Defendant's Data Breach.

74. As a condition of her employment with Defendant, Plaintiff Portee provided Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII/PHI in order to obtain employment and payment for that employment.

75. Plaintiff Portee provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain her PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

76. Plaintiff Portee reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

77. Plaintiff Portee received a Notice of Data Breach in November 2024.

78. Thus, on information and belief, Plaintiff Portee's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

79. Through its Data Breach, Defendant compromised Plaintiff Portee's PII/PHI.

80. Plaintiff Portee has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed her to take those steps in its breach notice.

81. And in the aftermath of the Data Breach, Plaintiff Portee has suffered from a spike in spam and scam phone calls since February 2024.

82. Plaintiff Portee fears for her personal financial security and worries about what information was exposed in the Data Breach.

83. Because of Defendant's Data Breach, Plaintiff Portee has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Portee's injuries are precisely the type of injuries that the law contemplates and addresses.

84. Plaintiff Portee suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

85. Plaintiff Portee suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

86. Plaintiff Portee suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed her PII/PHI right in the hands of criminals.

87. Because of the Data Breach, Plaintiff Portee anticipates spending considerable amounts of time and money to try and mitigate her injuries.

88. Today, Plaintiff Portee has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected

and safeguarded from additional breaches.

Plaintiff Jessie Ruiz-Jacobs's Experiences and Injuries

89. Plaintiff Ruiz-Jacobs is a former employee at Defendant.

90. As a condition of his employment at Defendant, he was required to provide Defendant with his sensitive PII, including his Social Security number.

91. Plaintiff Ruiz-Jacobs received a notice letter from Defendant dated November 19, 2024, informing him that his PII—including his Social Security number—was specifically identified as having been exposed to cybercriminals in the Data Breach.

92. Plaintiff Ruiz-Jacobs is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

93. At the time of the Data Breach, Defendant retained Plaintiff Ruiz-Jacobs's PII in its system.

94. Plaintiff Ruiz-Jacobs would not have provided his PII to Defendant had he known that Defendant would not utilize standard measures to reasonably secure his sensitive.

95. Because of the Data Breach, Plaintiff Ruiz-Jacobs's PII is now in the hands of cyber criminals. Plaintiff and all Class members are now imminently at risk of crippling future identity theft and fraud.

96. As a result of the Data Breach, Plaintiff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, researching how best to ensure that he is protected from identity theft, reviewing account statements and other information, and taking other steps in an attempt to mitigate the harm caused by the Data Breach.

97. Plaintiff Ruiz-Jacobs has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable PII; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's PII being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff's PII that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's PII; and (e) continued risk to Plaintiff's PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the PII that was entrusted to Defendant.

98. Plaintiff Ruiz-Jacobs further suffered actual injury in the form of experiencing fraudulent charges to his debit card, totaling approximately $80, in or about February 2024, which, upon information and belief, was caused by the Data Breach.

99. The Data Breach has caused Plaintiff Ruiz-Jacobs to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

100. As a result of the Data Breach, Plaintiff Ruiz-Jacobs anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

101. As a result of the Data Breach, Plaintiff Ruiz-Jacobs is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Peter Bungert's Experiences and Injuries

102. Plaintiff Bungert entrusted his PII to Defendant.

103. Plaintiff Bungert worked for Bojangles between 2014 and 2017.

104. Plaintiff Bungert received Defendant's Notice of Data Breach. The Notice stated that Plaintiff's PII, including his Social Security number and financial account information was impacted by the Data Breach.

105. As a result of the Data Breach, Plaintiff Bungert's sensitive information may have been accessed and/or acquired by an unauthorized actor. Defendant has not yet provided definitive findings for Plaintiff to know. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rests of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

106. As a result of the Data Breach, Plaintiff Bungert has spent time over 10 days – over 50 hours – dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

107. Additionally, Plaintiff Bungert is very careful about not sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

108. Plaintiff Bungert stores any documents containing his sensitive PII in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

109. Plaintiff Bungert has suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased

concern for the loss of his privacy.

110. Plaintiff Bungert has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

111. Plaintiff Bungert has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Christie Starnes' Experiences and Injuries

112. Plaintiff Lily Starnes is a former employee of Defendant.

113. Thus, Defendant obtained and maintained Plaintiff Starnes' PII/PHI.

114. As a result, Plaintiff Starnes was injured by Defendant's Data Breach.

115. As a condition of her employment with Defendant, Plaintiff Starnes provided Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII/PHI in order to obtain employment and payment for that employment.

116. Plaintiff Starnes provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain her PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

117. Plaintiff Starnes reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

118. Plaintiff Starnes received a Notice of Data Breach in November 2024.

119. Thus, on information and belief, Plaintiff Starnes' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

120. Through its Data Breach, Defendant compromised Plaintiff Starnes' PII/PHI.

121. Plaintiff Starnes has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed her to take those steps in its breach notice.

122. And in the aftermath of the Data Breach, Plaintiff Starnes has suffered from a spike in spam and scam phone calls since February 2024.

123. Plaintiff Starnes fears for her personal financial security and worries about what information was exposed in the Data Breach.

124. Because of Defendant's Data Breach, Plaintiff Starnes has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

125. Plaintiff Starnes suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

126. Plaintiff Starnes suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

127. Plaintiff Starnes suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed her PII/PHI right in the hands of criminals.

128. Because of the Data Breach, Plaintiff Starnes anticipates spending considerable

amounts of time and money to try and mitigate her injuries.

129. Today, Plaintiff Starnes has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Kassandra Blankenship's Experiences and Injuries

130. Plaintiff Kassandra Blankenship is a former employee of Defendant.

131. Thus, Defendant obtained and maintained Plaintiff Blankenship's PII/PHI.

132. As a result, Plaintiff Blankenship was injured by Defendant's Data Breach.

133. As a condition of her employment with Defendant, Plaintiff Blankenship provided Defendant with her PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII/PHI in order to obtain employment and payment for that employment.

134. Plaintiff Blankenship provided her PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain her PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

135. Plaintiff Blankenship reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

136. Plaintiff Blankenship received a Notice of Data Breach in November 2024.

137. Thus, on information and belief, Plaintiff Blankenship's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

138. Through its Data Breach, Defendant compromised Plaintiff Blankenship's PII/PHI.

139. Plaintiff Blankenship has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed her to take those steps in its breach notice.

140. And in the aftermath of the Data Breach, Plaintiff Blankenship has suffered from a spike in spam and scam phone calls since February 2024.

141. Plaintiff Blankenship fears for her personal financial security and worries about what information was exposed in the Data Breach.

142. Because of Defendant's Data Breach, Plaintiff Blankenship has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

143. Plaintiff Blankenship suffered actual injury from the exposure and theft of her PII/PHI—which violates her rights to privacy.

144. Plaintiff Blankenship suffered actual injury in the form of damages to and diminution in the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that Defendant was required to adequately protect.

145. Plaintiff Blankenship suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed her PII/PHI right in the hands of criminals.

146. Because of the Data Breach, Plaintiff Blankenship anticipates spending considerable amounts of time and money to try and mitigate her injuries.

147. Today, Plaintiff Blankenship has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Defendant's possession—is

protected and safeguarded from additional breaches.

Plaintiff James Higgins' Experiences and Injuries

148. Plaintiff James Higgins is, and at all times relevant has been, a resident and citizen of Concord, North Carolina. Plaintiff received a Notice of Data Breach letter (the "Notice Letter") dated November 19, 2024, on or about that date. The letter notified Plaintiff that his Private Information was among that compromised in the Data Breach. The type of data and information at issue included Plaintiff's name, Social Security number, financial account information, and medical information.

149. Plaintiff is a former employee of Defendant and as a condition of his employment he was required to provide Defendant with his Private Information. He did so on the mutual understanding that Defendant would reasonably safeguard his Private Information and use it only for necessary purposes within the scope of the employment relationship.

150. Plaintiff Higgins is not aware of any data breaches other than this one that exposed his Private Information and is concerned that it and other Private Information has now been exposed to bad actors.

151. As a result, he has taken multiple steps to avoid identity theft, including closely tracking his credit monitoring service, freezing and closing his accounts and carefully reviewing all his accounts. Plaintiff has already spent multiple hours dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

152. Plaintiff Higgins suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of privacy rights; and (c) present, imminent and impending injury arising

from the increased risk of identity theft and fraud.

153. As a result of the Data Breach, Plaintiff Higgins anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

154. Plaintiff greatly values his privacy, and would not have provided his Private Information, undertaken the services and paid the amounts that he did if he had known that his Private Information would be maintained using inadequate data security systems.

Plaintiff Leonardo Yon's Experiences and Injuries

155. Plaintiff Yon, a former employee of Defendant's, received a notification letter from Defendant informing him that he was a victim of Defendant's Data Breach.

156. Thus, at the time of the Data Breach, Defendant retained Plaintiff Yon's PII in its system.

157. Plaintiff Yon's PII was compromised in the Data Breach and stolen by identity thieves who illegally accessed Defendant's network for the specific purpose of targeting the PII.

158. Plaintiff Yon takes reasonable measures to protect his PII.

159. Plaintiff Yon suffered actual injury in the form of a severe privacy invasion because of his PII, including his Social Security number, falling into the hands of identity thieves whose mission it is to use that information to perpetrate identity theft and financial fraud.

160. Plaintiff suffered lost time, interference, and inconvenience because of the Data Breach and has experienced stress and anxiety due to increased concerns for the loss of his privacy and because he knows he must now face a substantial increase in identity theft and financial fraud attempts for years to come.

161. Plaintiff Yon has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his name and Social Security number, being placed in the hands of criminals whose mission it is to misuse that data.

162. Defendant obtained and continues to maintain Plaintiff Yon's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff's PII was compromised and disclosed because of the Data Breach.

163. Because of the Data Breach, Plaintiff Yon anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Yon is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

164. In addition to the significantly increased risk of identity theft and financial fraud that Plaintiff Yon must now face because of Defendant's failures, and in additional to the significant invasion of his privacy.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

165. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from

identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII/PHI.

166. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII/PHI can be worth up to $1,000.00 depending on the type of information obtained.

167. The value of Plaintiffs and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

168. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

169. One way that criminals profit from stolen PII/PHI is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII/PHI, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

170. The development of "Fullz" packages means that the PII/PHI exposed in the Data

Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

171. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

172. Defendant disclosed the PII/PHI of Plaintiffs and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII/PHI of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

173. Defendant's failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

174. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

175. In 2021, a record 1,862 data breaches occurred, exposing approximately

293,927,708 sensitive records—a 68% increase from 2020.[16]

176. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[17]

177. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

178. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

179. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[18] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

---

[16] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[17] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[18] *Protecting Personal Information: A Guide for Business,* FED TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

180. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

181. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

182. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

183. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

184. Several best practices have been identified that—at a *minimum*—should be

implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

185. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

186. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

187. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

Defendant Violated HIPAA

188. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic

transactions and code sets to maintain the privacy and security of protected health information.[19]

189. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII/PHI and PHI is properly maintained.[20]

190. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

[19] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[20] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

191. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

192. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Bojangles'

> Restaurants, Inc. in February 2024, including all those individuals who received notice of the breach.

193. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

194. Plaintiffs reserve the right to amend the class definition.

195. Certification of Plaintiffs claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

196. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

197. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 100 members.

198. Typicality. Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

199. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class Members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

200. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting

individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII/PHI;

b. if Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII/PHI;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

201. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for

their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

202. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

203. Plaintiffs and the Class entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their PII/PHI to unauthorized third parties.

204. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

205. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiffs and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

206. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class Members' PII/PHI.

207. Defendant owed—to Plaintiffs and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their PII/PHI.

208. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

209. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

210. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

211. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII/PHI, a

necessary part of obtaining services from Defendant.

212. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

213. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiffs and Class Members' and the importance of exercising reasonable care in handling it.

214. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

215. Defendant breached these duties as evidenced by the Data Breach.

216. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII/PHI by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

217. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs and Class Members' injury.

218. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class Members' injuries-in-fact.

219. Defendant has admitted that the PII/PHI of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

220. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

221. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

222. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class)

223. Plaintiffs incorporate by reference paragraphs1 through 180 above as if fully set forth herein.

224. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate

computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII/PHI.

225. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class Members' sensitive PII/PHI.

226. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

227. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

228. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

229. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class Members would not have been injured.

230. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known

that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

231. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class Members' PHI.

232. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

233. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

234. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

235. Plaintiffs incorporate by reference paragraphs 1 though 180 above as if fully set forth herein.

236. Plaintiffs and Class Members were required to provide their PII/PHI to Defendant as a condition of receiving employment provided by Defendant. Plaintiffs and Class Members provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's employment.

237. Plaintiffs and Class Members reasonably understood that a portion of the funds derived from their labor would be used to pay for adequate cybersecurity measures.

238. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

239. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for employment.

240. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

241. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII/PHI.

242. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

243. After all, Plaintiffs and Class Members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

244. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

245. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their

contract in addition to its form.

246. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

247. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

248. In these and other ways, Defendant violated its duty of good faith and fair dealing.

249. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

250. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

251. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

252. Plaintiffs incorporate by reference paragraphs 1 though 180 above as if fully set forth herein.

253. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

254. Defendant owed a duty to its current and former employees, including Plaintiffs and the Class, to keep this information confidential.

255. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' PII/PHI is highly offensive to a reasonable person.

256. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

257. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

258. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

259. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation

efforts.

260. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

261. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

262. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

263. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

264. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiffs and the Class.

265. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

266. Plaintiffs incorporate by reference paragraphs 1 though 180 above as if fully set forth herein.

267. This claim is pleaded in the alternative to the breach of implied contract claim.

268. Plaintiffs and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII/PHI to facilitate employment, and (2) using their labor to derive profit.

269. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members.

270. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

271. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII/PHI.

272. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

273. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' (1) PII/PHI and (2) employment because Defendant failed to adequately protect their PII/PHI.

274. Plaintiffs and Class Members have no adequate remedy at law.

275. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

SIXTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

276. Plaintiffs incorporate by reference paragraphs 1 through 180 above as if fully set forth herein.

277. Given the relationship between Defendant and Plaintiffs and Class Members, where Defendant became guardian of Plaintiffs' and Class Members' PII/PHI, Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' PII/PHI; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

278. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII/PHI.

279. Because of the highly sensitive nature of the PII/PHI, Plaintiffs and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII/PHI had they known the reality of Defendant's inadequate data security practices.

280. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class Members' PII/PHI.

281. Defendant also breached its fiduciary duties to Plaintiffs and Class Members by

failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

282. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

SEVENTH CAUSE OF ACTION
Violation of North Carolina Unfair and Deceptive Trade Practices Act
(On Behalf of Plaintiffs and the Class)

283. Plaintiffs incorporate by reference paragraphs 1 through 180 as if fully set forth herein.

284. The North Carolina Unfair and Deceptive Trade Practices Act provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful." G.S. § 75-1.1.

285. Defendant violated the North Carolina Unfair and Deceptive Trade Practices Act by, *inter alia*:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII/PHI, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII/PHI, including

duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*., which was a direct and proximate cause of the Data Breach;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII/PHI; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII/PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

286. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of their PII/PHI.

287. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its omissions.

288. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure—and thus vulnerable to attack—Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII/PHI that Plaintiffs and Class Members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class Members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

289. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded Plaintiffs' and Class Members' rights.

290. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII/PHI.

291. And, on information and belief, Plaintiffs' PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

292. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law.

EIGHTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

293. Plaintiffs incorporate by reference paragraphs 1 through 180 as if fully set forth herein.

294. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

295. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs

and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

296. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class Members.

297. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

298. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

299. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs' and Class Members' injuries.

300. If an injunction is not issued, the resulting hardship to Plaintiffs and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

301. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiffs, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further unfair and/or deceptive practices;

E. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: January 30, 2025

Respectfully submitted,

By: /s/ *Scott C. Harris*

Scott C. Harris
N.C. State Bar No.: 35328
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W. Morgan St.
Raleigh, NC 27603
Telephone: (919) 600-5003
Fax: (919) 600-5035
sharris@milberg.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Ft. Lauderdale, FL 33301
T: (954) 525-4100
ostrow@kolawyers.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Marc H. Edelson*
EDELSON LECHTZIN LLP
411 S. State Street, Suite N300
Newton, PA 18940
T: (215) 867-2399
medelson@edelson-law.com

Nicholas A. Migliaccio*
Jason Rathod*
MIGLIACCIO & RATHOD LLP
412 H Street NE
Washington, D.C. 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

J. Gerard Stranch, IV*
Grayson Wells*
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Tel: (615) 254-8801
gstranch@stranchlaw.com
gwells@stranchlaw.com

William B. Federman*
Jessica A. Wilkes*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Tel: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081
wbf@federmanlaw.com
jaw@federmanlaw.com

Terence R. Coates*
Spencer D. Campbell*
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
scampbell@msdlegal.com

**Pro hac vice forthcoming*

Attorneys for Plaintiffs and Proposed Class